



## Information Technology

Sarah Edgerton, Chief Information Officer

City-County Building, Room 500

210 Martin Luther King, Jr. Blvd.

Madison, WI 53703

Phone: (608) 266-4454 | Fax: (608) 261-9289

[it@cityofmadison.com](mailto:it@cityofmadison.com)

[cityofmadison.com/information-technology](http://cityofmadison.com/information-technology)

February 11, 2019

Matt Chapman

Free Our Info, NFP

MuckRock News

E-mail: [68175-16903250@requests.muckrock.com](mailto:68175-16903250@requests.muckrock.com)

RE: *Request for Email Metadata (Information Technology)*

Dear Mr. Chapman,

Thank you for your recent email in which you requested:

*For all email accounts under the management of this city, please provide me the following information for all emails sent and received during January, 2019:*

- 1. From address*
- 2. To address*
- 3. bcc addresses*
- 4. cc addresses*
- 5. Time*
- 6. Date*

Your request is respectfully denied. The City does not maintain a record containing the information you have requested, nor can the City identify any business purpose for creating such a record. To the extent that a report could be compiled, Records Custodians incur no obligation to create a record in order to satisfy a requestor's query per Wis. Stats. §19.35(1)(L).

Further, if a report were to be compiled, due diligence would require the City to review each of the approximately 50,000 daily email data entries for confidential material. We would need to read the content of each email to determine whether it is necessary to redact any email addresses that would disclose law enforcement confidential informants, other cooperating individuals, information identifying attorney-client communications and confidential health related communications. In many instances, it is not merely the contents of the communications that are privileged, but also the very fact that a communication occurred and the circumstances surrounding those communications.

The City maintains several notification lists where participants may elect (in accordance with CAN-SPAM Act) to keep their email addresses confidential. Releasing those email addresses to you would not only undermine the public's confidence that the City will abide by their requests for confidentiality, it could

also be illegal.

City employees are permitted incidental personal use of the City's email system. The Wisconsin Supreme Court has determined that such personal email communications are exempt from disclosure under the Wisconsin Public Records Laws, *Schill v. Wisconsin Rapids Sch. Dist.*, 2010 WI 86. The Court did not distinguish between the headers of the email and the content of the email, but rather, it held that the entire personal communications were exempt from disclosure. Therefore, all email addresses gleaned from personal communications would need to be redacted from the report that you have requested, and there is no practical way to identify and redact such personal information.


The paragraphs above detail only some of the due diligence review necessary before releasing such a report. Efforts to accomplish its due diligence would easily overwhelm the City's available resources. Such efforts are simply not practical nor achievable. Therefore, the request is considered to be overly broad and unduly burdensome. "A request for a record without reasonable limitation as to subject matter or length of time does not constitute a sufficient request. A request can be denied if it is too burdensome and the requester could have limited the request but failed to do so. Section 19.35(1)(h), Wis. Stats.; *Schopper v. Gehring*, 210 Wis.2d 208, 565 N.W.2d 187 (Ct. App. 1997)," Understanding the Wisconsin Public Records an Open Meetings Laws, State Bar of Wisconsin, December 1999.

Additionally, using the requested metadata, malicious actors could employ several forms of social engineered attack vectors which could result in gaining access to City of Madison resident's, employee's or partner's sensitive data, including personal or financial information, or trade secrets. The City of Madison cybersecurity team has identified several ways this data could be used to facilitate these types of attacks. Some common examples include email-based DDOS, Quid Pro Quo, Piggybacking, Spear/Whale Phishing (Authority), CEO Fraud, Pharming, Drop Box Phishing or Google Docs Phishing.

The presumption of openness in the public records laws is based upon the principle that "representative government is dependent upon an informed electorate" and therefore, the public is entitled to access the records documenting "the affairs of government and the official acts of those officers and employees who represent them." (Wis. Stats. §19.31) However, the report that you have asked us to create provides no substantive information about the affairs of government or official acts of government officers/employees and thus, does not advance the purpose of the public records laws.

Your request is denied for each of the foregoing reasons. Pursuant to section 19.35(4)(b) of the Wisconsin Statutes, I advise you that this determination is subject to review by mandamus under section 19.37(1) of the Wisconsin Statutes, or upon application to the Attorney General or Dane County District Attorney.

Respectfully,



Sarah Edgerton, Director  
City of Madison Information Technology

cc: Paul R. Soglin, Mayor  
Michael P. May, City Attorney